EFFICIENT, FAULT-TOLERANT AND DISTRIBUTED KEY AGREEMENT FOR ARBITRARY DEPLOYMENT IN MANETS

Giovanni Di Crescenzo
Telcordia Technologies Inc.
Piscataway, NJ, 08854

Maria Striki
Electrical and Computer Engineering
and the Institute of Systems Research
University of Maryland, College Park, MD, 20740

ABSTRACT

Military command and control require that information be communicated to the appropriate groups and only with the utmost security. The environment envisioned by the Objective Force is mobile ad-hoc and consists of a large number of (heterogeneous) resource-constrained nodes deployed in a hostile field of limited bandwidth, unreliable channels, frequent node failures, where usually there is not infrastructure for communications, and it must be dynamically generated. The challenge lies in designing secure group communications that can be applied to such dynamic, constrained FCSs. In this work we develop a secure, fault-tolerant and scalable (for increasing number of users) contributory *key agreement scheme* (KA) for multicast communications. By generating **hierarchy,** applying **improved** and **more resilient** contributory protocols to **smaller subsets** of nodes**,** focusing on the **exact topology** of nodes deployed in the network**,** and by exploiting the **redundancy** issued by the **topology** itself, we **successfully** meet our **objectives.** Our protocol – **Clustered Local Contributory (CLC)** - is secure (against eavesdropping adversaries), captures the dynamics of subgroups, it is highly fault-tolerant and very efficient in terms of communication and computation overhead. According to the results of the comparative evaluation of CLC and some of the most common contributory protocols in the literature (e.g. GDH.2) we conducted, it appears that CLC presents **superior performance** in terms of communication, computation and storage overhead incurred to the network in order to secure group communications in MANETs.

1. INTRODUCTION

Most of the existing key generation (KG) schemes rely upon assumptions that generally do not hold in the MANETs we are considering: e.g. all participants of the key management (KM) group can be reached with a single broadcast, the routing is considered reliable and secure, there exist centralized entities that facilitate the desired group operations, nodes have global view of the network graph and can thus easily synchronize operations. Our KA protocol is not based on unrealistic assumptions similar to the above. Based on local information only, it captures the arbitrary nature of nodes' deployment in the network, and adapts the KA function to the particular deployment, rather than adjusting the deployment to the topological structure and the requirements of a given KA protocol as is usually the case in the literature. Furthermore, existing KA protocols usually isolate the logical design from network operations and phases that are required prior to the execution of the actual KA. They do not deal with the collection of the appropriate group or topology information, with establishing communication links, or with issues of sequence and synchronization. In MANETs, and for a growing number of users, these tasks become particularly hard to accommodate. This is the reason why many new protocols that follow the above design pattern and are proposed for MANETs fail, since they cannot scale to a large number of nodes. Ours instead, is a KA scheme that focuses on the actual topology, and utilizes simple clustering to tackle scalability and coordinate nodes locally and thus more effectively and efficiently in an environment of minimal resources and information, e.g. battlefield. It can be applied to dynamically changing environments (e.g. MANETs), where most of the assumptions of other protocols fail to be met.

2. MODEL AND ASSUMPTIONS

The entities of the KA group are represented as the vertices V in a (not necessarily connected) graph G:$\{V,E\}$. An edge is attributed between two vertices, representing a communication link, if and only if the associated two entities are within radio range of each other. In this scenario, as could also be the case in a secret army squad, each entity knows the IDs of the rest of the participants, but this constraint may also be relaxed. We assume that all nodes participating to the KA process are honest, but consider node failures, due to crashes or mobility, and model them using node and edge failures in G. An adversary is allowed to eavesdrop on the entire communication along the graph; Byzantine adversaries will be addressed in future work. Thus, routing within paths on G (only among members of the group) is considered reliable (when connectivity is superior to the number of crashes).

Prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U.S. Army Research Laboratory under the Collaborative Technology Alliance (CTA) Program, Cooperative Agreement DAAD19-2-01-0011. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
00 DEC 2004	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Efficient, Fault-Tolerant And Distributed Key Agreement For Arbitrary Deployment In Manets	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Telcordia Technologies Inc. Piscataway, NJ, 08854; Electrical and Computer Engineering and the Institute of Systems Research University of Maryland, College Park, MD, 20740**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001736, Proceedings for the Army Science Conference (24th) Held on 29 November - 2 December 2005 in Orlando, Florida. , The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**2**	

3. CLUSTERED LOCAL CONTRIBUTORY ALGORITHM (CLC)

We distinguish the following phases of our KA scheme that applied sequentially, achieve the establishment of a common group key through all nodes in the network in an efficient and totally distributed manner:

P1: Neighbor Discovery and Subgroup Leader Election: Initially, 1-hop neighbors exchange their IDs and network information through "Hello" messages. Nodes collect these messages, and each broadcasts to its 1-hop neighbors the IDs and certain metrics of interest of all its 1-hop neighbors. In the end, all nodes have a local view of a 2-hop depth network sub-graph, and select either a 1-hop or 2-hop neighbor as their subgroup leader, based on the given metrics, and notify it of their decision.

P2: Subgroups Formation: In the case of 1-hop leader selection, a node selected by other nodes as subgroup leader, either becomes leader indeed, or delegates the leadership to its own leader selection, as long as all nodes involved in the new subgroup are not more than 2-hops away from the new leader. Similar is the algorithm for the 2-hop leader selection. Leaders notify nodes that have selected them of the current status.

P3: Subgroups adjusted to Robustness Requirement (RR): A subgroup is classified as reliable or unreliable depending on whether it acquires at least ***t*** border nodes that directly reach at least one among the neighbor subgroups (RR). If a 1-hop subgroup does not meet RR, it will be merged with another subgroup in P2, if possible. Otherwise, P3 is used for readjustments so that more subgroups can meet RR.

P4-1: Establishment of a common subgroup key within each individual subgroup: In this phase, a common key is generated among subgroup nodes. The protocols applied within the subgroups are DH-based but modified w.r.t. the individual sub-graph configuration resulting after the subgroup formation, and they are more efficient and resilient to failures.

P4-2: Overlay Modified Spanning Tree Algorithm (OMST): This phase may run in parallel with P4-1. As soon as the subgroup leader and neighbor subgroups are known, one pre-defined subgroup (e.g. lower leader ID) initiates OMST. This algorithm places all connected subgroups as vertices in a virtual overlay tree. It provides an orderly way of group key establishment from subgroup keys via a *tree* KA scheme, considering the classification of subgroups into strongly (reliable) and weakly (unreliable) connected, while building the tree. In case of any link failures, the communication is recovered (unless there is a total partition) with the least possible overhead.

P5: Group Key Establishment with OMST: All keys of subgroups that are not disconnected from the group, are combined to construct the overall group key.

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied of the Army Research Laboratory or the U.S. Government

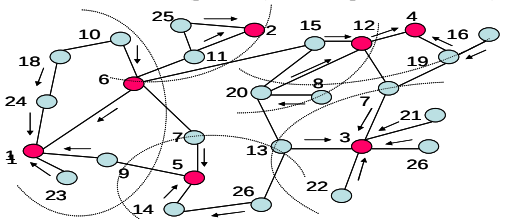
Each subgroup notifies its neighbor subgroups that it successfully completed P4-1, for the synchronization of group KA. The border nodes of each subgroup send their subgroup key to the subgroup(s) designated by OMST and so on and so forth, until the root of the virtual tree is reached and the group key is computed. Following the tree backwards and sending the appropriate key shares to each subgroup, the group key can be reconstructed from all subgroups and subsequently from all group nodes.

4. DISCUSSION AND PERFORMANCE

CLC seems to be a very good fit for the battlefield, where few assumptions can be made, and soldiers rely on their own resources to reach their comrades and establish secure, robust and low cost group communication. Failures and mobility changes are first handled locally within the associated subgroup, and only if needed, status information is propagated to the rest via OMST, to restore the group. The option of reliable routing on the graph paths may also be exploited from OMST, border nodes, subgroup leaders, or in cases of node failures. We compared CLC with GDH.2 KA protocol for the same topology configurations. We find through analytical evaluation and simulations that CLC is more efficient in terms of the communication and computation overhead issued, and far more resilient to failures. The following table shows roughly the results of the comparison of applying CLC vs. "blind" GDH.2 to all the nodes (n=27) in the random graph of the scheme, for phases 4, 5.

Protocol (n=27)	CLC P4-1	CLC P4-2+P5	CLC P4, 5	GDH.2
Comm/tion msg.	<80	<90	<170	415 (comb)
Computation exps.	<120	<40	<160	404

Table 1: Communication (packets) & Computation Cost (exp/s)



CONCLUSIONS

We have designed a distributed KA protocol for MANETs - CLC - that is secure, fault-tolerant, efficient and scalable. In particular, the introduction of hierarchy to the network, the use of more efficient protocols within the subgroups and the ability to constructively use neighbor information are key factors for dramatic reduction of communication-computation costs, and improvement in resiliency.

REFERENCES

Steiner, M., Tsudik, G., Waidner, M., "Diffie-Hellman Key Distribution Extended to Groups", 3rd ACM conference on Computer/Comm/tions Security, ACM Press, 1996, 31-37